IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for analyzing a network protocol stream for a security-related event, comprising:

identifying at least two valid states associated with a network protocol in which a first host system communicating with a second host system using the network protocol may be placed;

defining at least one valid transition between a first state of the at least two valid states and a second state of the at least two valid states;

expressing the at least one valid transition in the form of a first regular expression;

defining an invalid state associated with the network protocol;

expressing a plurality of invalid transitions from the first state to the invalid state as a plurality of regular expressions, the plurality of invalid transitions being direct transitions from the first state to the invalid state;

determining that a connection under the network protocol is in the first state; and

applying to a received packet associated with the connection:

the first regular expression to determine whether the packet is associated with the at least one valid transition, and

the plurality of regular expressions to determine whether the packet is associated with one of a plurality of invalid transitions; and

in the event it is determined by applying the plurality of regular expressions to the packet that the packet is associated with a particular one of the plurality of invalid transitions, taking a corresponding responsive action associated specifically with the particular one of the plurality of invalid transitions.

2. (Previously Presented) A method for analyzing a network protocol stream as recited in claim 1, further comprising compiling the first regular expression into computer code.

3. (Original) A method for analyzing a network protocol stream as recited in claim 2, wherein the computer code comprises code in the C programming language.

4. (Original) A method for analyzing a network protocol stream as recited in claim 2, wherein the computer code comprises optimal computer code.

5. (Original) A method for analyzing a network protocol stream as recited in claim 2, wherein the computer code comprises nearly optimal computer code.

6. (Previously Presented) A method for analyzing a network protocol stream as recited in claim 1, wherein using the first regular expression to analyze the network protocol stream comprises copying the network protocol stream to a third system and using the first regular expression to analyze the network protocol steam at the third system.

7. (Original) A method for analyzing a network protocol stream as recited in claim 6, wherein the network protocol stream comprises packets of data, each packet being associated with a sequence number indicating its position relative to other packets in the protocol stream, and the third system reassembles the packets into the order indicated by the respective sequence numbers of the packets received.

8. (Original) A method for analyzing a network protocol stream as recited in claim 7, wherein a copy of the network protocol stream is maintained in the third system until analysis has been completed.

9. (Original) A method for analyzing a network protocol stream as recited in claim 7, wherein in the event the packets are received by the third system in sequence number order, a copy is maintained in the third system only of those packets comprising the portion of the network protocol currently under analysis.

10. (Previously Presented) A method for analyzing a network protocol stream as recited in claim 1, further comprising keeping track of which of the at least two valid states the first host system currently is in.

11. (Previously Presented) A method for analyzing a network protocol stream as recited in claim 10, further comprising changing the tracked state of the first host system from the first of the at least two valid states to the second of the at least two valid states in the event the analysis of the network protocol stream indicates the at least one valid transition has taken place.

12. (Cancelled)

13. (Previously Presented) A method for analyzing a network protocol stream as recited in claim 1, wherein the invalid transition indicates that a security-related event has taken or is taking place.

14. (Cancelled)

15. (Previously presented) A method for analyzing a network protocol stream as recited in claim 1, further comprising:

keeping track of which state, from the set comprising the at least two valid states and the invalid state, the first host system currently is in; and

changing the state of the first host system to the invalid state in the event that the analysis of the network protocol stream indicates the invalid transition has taken place.

16. (Previously presented) A method for analyzing a network protocol stream as recited in claim 15, further comprising providing, in the event that the analysis of the network protocol stream indicates the invalid transition has taken place, an indication that the invalid transition has taken place.

17. (Previously presented) A method for analyzing a network protocol stream as recited in claim 15, further comprising discontinuing analysis of the network protocol stream once the state of the first host system has been changed to the invalid state.

18. (Cancelled)

19. (Currently Amended) A system for analyzing a network protocol stream between a first host system and a second host system for a security-related event, the first host system being susceptible to being placed under the network protocol in one of at least two valid states associated with the network protocol, the system comprising:

a computer configured to:

receive a network protocol stream;

determine that a connection under the network protocol is in a first state of the at least two valid states; and

apply to a received packet associated with the connection:

a first regular expression corresponding to a valid transition from the first state of the at least two valid states to a second state of the at least two states, and

a plurality of regular expressions corresponding to a plurality of invalid transitions from the first state of the at least two valid states to a predefined, invalid state, the plurality of invalid transitions being direct transitions from the first state to the invalid state; and

in the event it is determined by applying the plurality of regular expressions to the packet that the packet is associated with a particular one of the plurality of invalid transitions, take a corresponding responsive action associated specifically with the particular one of the plurality of invalid transitions; and

a memory associated with the computer and configured to store the first regular expression.

20. (Currently Amended) A system for analyzing a network protocol stream between a first host system and a second host system for a security-related event, the first host system being susceptible to being placed under the network protocol in one of at least two valid states associated with the network protocol, the system comprising:

means for receiving the network protocol stream; and

means for analyzing the network protocol stream by:

determining that a connection under the network protocol is in a first state of the at least two valid states;

applying to a received packet associated with the connection:

a first regular expression corresponding to a valid transition from the first state of the at least two valid states to a second state of the at least two valid states; and

a plurality of regular expressions, the plurality of regular expressions corresponding to a plurality of invalid transitions from the first state of the at least two valid states to a pre-defined, invalid state, the plurality of invalid transitions being direct transitions from the first state to the invalid state; and

in the event it is determined by applying the plurality of regular expressions to the packet that the packet is associated with a particular one of the plurality of invalid transitions, taking a corresponding responsive action associated specifically with the particular one of the plurality of invalid transitions.

21. (Currently Amended) A computer program product for analyzing a network protocol stream, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

identifying at least two valid states in which a first host system communicating with a second host system using a network protocol may be placed;

defining at least one valid transition between a first state of the at least two states and a second state of the at least two valid states;

expressing the at least one valid transition in the form of a first regular expression;

defining an invalid state associated with the network protocol;

expressing a plurality of invalid transitions from the first state to the invalid state as a plurality of regular expressions, the plurality of invalid transitions being direct transitions from the first state to the invalid state;

determining that a connection under the network protocol is in the first state; and

applying to a received packet associated with the connection:

the first regular expression to determine whether the packet is associated with the at least one valid transition, and

the plurality of regular expressions to determine whether the packet is associated with one of a plurality of invalid transitions; and

in the event it is determined by applying the plurality of regular expressions to the packet that the packet is associated with a particular one of the plurality of invalid transitions, taking a corresponding responsive action associated specifically with the particular one of the plurality of invalid transitions.

22. (Cancelled)

23. (Cancelled)

24. (Previously Presented) A method as recited in Claim 1, wherein some of the plurality of regular expressions are grouped according to their similarity into adjacent positions for packet processing.

25. (Previously Presented) A method as recited in Claim 1, wherein the plurality of invalid transitions correspond to a plurality of disallowed security events.

26. (Previously Presented) A method as recited in Claim 1, wherein the plurality of invalid transitions correspond to a plurality of disallowed security events; and in the event that the packet is associated with one of the plurality of invalid transitions, the method further comprising performing error handling based on a disallowed security event that corresponds to said one of the plurality of invalid transitions.